

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG. 5462

In the Matter of Warrants for All Content
and Other Information Associated with the
Email Accounts: Bsweet002@yahoo.com,
Cholder@aol.com, and
Jeff.wada@gmail.com, Maintained
Respectively at Premises Controlled by
Yahoo!, Inc., AOL, and Google, Inc.
USAO Reference No. 2017R00493

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for Search Warrants
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

LYESON DANIEL, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Postal Inspector with the United States Postal Inspection Service for approximately 1 year, where I am assigned to a squad responsible for investigating white collar crime, including securities fraud and accounting fraud. I have received training regarding computer technology and in the execution of search warrants involving electronic documents. Prior to joining the United States Postal Inspection Service, I was employed for approximately 7 years in the civil enforcement division of the New York State Department of Taxation and Finance, where I conducted and supervised investigations into corporate financials in order to determine whether taxes had been properly paid. In addition, I have a bachelor's degree in information (computer) systems and a masters degree in accounting.

B. The Providers, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts (i) Bsweet002@yahoo.com (the “Sweet Account”), maintained and controlled by Yahoo!, Inc., headquartered at 701 First Avenue, Sunnyvale, California 94089; (ii) Cholder@aol.com (the “Holder Account”) maintained and controlled by AOL, headquartered at 770 Broadway, New York, New York; and (iii) Jeff.wada@gmail.com (the “Wada Account” and together with the Sweet and Holder Accounts, the “Subject Accounts”) maintained and controlled by Google, Inc. (together with Yahoo! and AOL, the “Providers”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrants.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of Title 15, United States Code, Sections 7202(b)(1) & 78ff and Ethics Code 9 of the Rules of the Public Company Accounting Oversight Board (the “PCAOB”) (willful violations of PCAOB Rules constituting criminal violations of the Securities Exchange Act of 1934); Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Sections 1346 and 1343 (honest services wire fraud); Title 18, United States Code, Section 1503 (obstruction of justice); Title 18, United States Code, Section 1519 (destruction, alteration or falsification of records to obstruct a government investigation); conspiracy to commit such offenses in violation of Title 18, United States Code, Section 371; and aiding and abetting such offenses in violation of Title 18, United States Code, Section 2 (together, the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, information provided by counsel for KPMG (“KPMG Counsel”) and counsel for the PCAOB (“PCAOB Counsel”) based on, among other things, their respective

internal investigations and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Providers

4. I have learned the following about the Providers:

a. The Providers offer email services to the public. In particular, the Providers allow subscribers to maintain email accounts under the respective domain names yahoo.com, aol.com, and gmail.com, among others. A subscriber using the Providers' services can access his or her email account from any computer connected to the Internet.

b. The Providers maintain the following records and information with respect to every subscriber account, among others:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Providers' servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Providers' computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Providers' servers for a certain period of time.

ii. *Address book.* The Providers also allow subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Providers collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Providers also maintain records concerning the date on which the account was created, the Internet protocol (“IP”) address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Providers maintain records of the subscriber’s means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* The Providers also typically retain certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Providers’ website).

v. *Customer correspondence.* The Providers also typically maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

vi. *Preserved and backup records.* The Providers also maintain preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Providers may also maintain backup copies of the foregoing categories of records pursuant to their own data retention policy.

vii. *Browser History.* With respect to every subscriber/email account, Google maintains a web history, that is, searches and account browsing activity, from Chrome, Google’s proprietary web browser, as well as other of Google’s applications.

D. Jurisdiction and Authority to Issue Warrants

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Providers, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated,” 18 U.S.C. § 2711(3)(A)(i), and/or “is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(ii).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Providers from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

8. Based on information provided by KPMG Counsel and PCAOB Counsel, including information derived from their respective internal investigations, my own participation in witness interviews, my review of documents, including emails, text messages, and personnel files, and other information, I know the following:

The PCAOB and Its Employees

9. In general, in order to register securities with the Securities and Exchange Commission (“SEC”), a public company must disclose annual audited financial statements. These financial statements are audited by an independent certified public accountant (an “Auditor”) who examines the company’s financial statements and other documentation in order to ascertain whether the financial statements are accurate, truthful, and complete pursuant to Generally Accepted Accounting Principles (“GAAP”). After completing an examination of a company’s financial statements, an Auditor issues a written report or “audit report” as to whether the financial statements are fairly stated and comply in all material respects with GAAP. An Auditor must complete its review of the financial statements prior to issuing its audit report, but may document previously completed work within the 45-day period following the issuance of the audit report (the “Documentation Period”). After the conclusion of the Documentation Period, an Auditor is generally prohibited from altering or adding to its work papers for a given audit.

10. The Public Company Accounting Oversight Board (the PCAOB or the “Board”) is a nonprofit organization created by the Sarbanes-Oxley Act of 2002 (“SOX”) and modelled after self-regulatory organizations in the securities industry that investigate and discipline their own members, subject to oversight by the SEC. Among other responsibilities, the PCAOB inspects registered public accounting firms to assess compliance with various auditing and accounting rules and standards, as set forth in SOX, rules promulgated by the SEC and the PCAOB, and other professional standards in connection with accounting firms’ performance of audits and issuance of audit reports, among other matters.

11. SOX commands that the rules of the PCAOB (the “PCAOB Rules”), among other things, establish ethics rules and standards of conduct for Board members and staff. The PCAOB

Rules are subject to the approval of the SEC. SOX also provides that a violation of PCAOB rule shall be treated as a violation of the Securities Exchange Act of 1934 (the “Exchange Act”) or rules issued pursuant to the Exchange Act, and that any person violating PCAOB Rules will be subject to the same penalties applied to a violation of the Exchange Act.¹ One rule promulgated by the PCAOB as part of its ethics code and approved by the SEC, is Ethics Code 9 (“EC 9”), which is entitled “Nonpublic Information.” EC 9 states:

Unless authorized by the Board, no Board member or staff shall disseminate or otherwise disclose any information obtained in the course and scope of his or her employment, and which has not been released, announced, or otherwise made available publicly. The provisions of this Section shall continue in effect after the termination of employment or Board membership.

12. The PCAOB conducts inspections of registered accounting firms pursuant to two programs: (i) the Global Network Firm (“GNF”) program, which inspects the 6 largest United States Accounting firms and their global affiliates; and (ii) a second program for all other firms. KPMG is one of the 6 largest accounting firms, and accordingly, is inspected as part of the GNF program. The PCAOB maintains a dedicated team of inspectors for each of the firms in the GNF program. In order to determine which of KPMG’s engagements to inspect in a particular year, the PCAOB’s inspection team receives a list of all audits conducted by KPMG the prior year, and certain data about each audit. Typically, in or around November and December of each year, the PCAOB selects which of KPMG’s audits are to be inspected. It does so based on a variety of factors including how long it has been since a particular engagement was inspected, the risk factors for the audit, and an interest in including some randomly selected engagements, among others.

¹ Willful violations of the Exchange Act or rules issued under the Exchange Act are subject to criminal prosecution. *See* 15 U.S.C. § 78ff.

13. The PCAOB generally notifies an accounting firm of an inspection approximately 2 to 4 weeks before the inspection is to take place, but in no event prior to the completion of the Documentation Period for that audit. This is because it is important to the PCAOB that it inspect a firm's actual audit work on an engagement, and not additional work done by a firm because of a known upcoming inspection. Accordingly, the internal list maintained by the PCAOB regarding its planned intended upcoming inspections is high confidential.

14. Once a PCAOB inspection is complete, and following an opportunity for the accounting firm to contest any findings, the PCAOB issues an Inspection Report (the "Report"). The Report contains two parts. Part I, which is publicly available, documents instances in which the PCAOB found that the auditor failed to gather sufficient audit evidence to support an audit opinion. Part II, which is not public, relates to any defects or systemic deficiencies noted in the inspection. An accounting firm is given one year to remedy any deficiencies noted in Part II, after which time, if the deficiencies are not corrected, the Part II form is made public. The number of "comments," (a term of art for negative findings) received by a firm in both Part I and Part II is publicly available, and accounting firms strive to avoid such comments.

Relevant PCAOB Personnel

15. Between approximately 2009 and approximately April 24, 2015, Brian Sweet ("Sweet") was an employee of the PCAOB. At the time Sweet left the PCAOB, he was an Associate Director with the PCAOB.

16. Between approximately December 2011 and approximately July 2015, Cynthia "Cindy" Holder ("Holder") was an employee of the PCAOB. At the time Holder left the PCAOB, she was an Inspections Leader with the PCAOB.

17. Between approximately 2004 and approximately 2017, Jeffrey Wada (“Wada”) was an employee of the PCAOB. At the time Wada left the PCAOB, he was an Inspections Leader with the PCAOB.

18. The PCAOB regularly trains its employees on applicable laws and PCAOB Rules. While employed at the PCAOB, Sweet, Holder and Wada each signed certifications agreeing to abide by such rules, including, but not limited to EC 9.

Relevant KPMG Personnel

19. On or about May 4, 2015, Sweet began working at KPMG as an Audit Partner in the Department of Professional Practice – Inspections.

20. On or about August 1, 2015, Holder began working at KPMG as an Executive Director in Risk and Regulatory, Department of Professional Practice – Inspections.

21. At all relevant times David Britt (“Britt”) was an Audit Partner in the Department of Professional Practice, Banking and Capital Markets.

22. At all relevant times, George Hermann (“Hermann”), was a KPMG Audit Partner in the Audit Quality and Professional Practice Group and held the title of Chief Auditor.

23. At all relevant times, Scott Marcello (“Marcello”) was a KPMG Audit Partner and, as of July 2015, was also the Vice Chair of Audit.

24. At all relevant times, David Middendorf (“Middendorf”) was KPMG’s National Managing Partner for the Audit Quality and Professional Practice Group.

25. At all relevant times Thomas Whittle (“Whittle”) was a KPMG Audit Partner in the Audit Quality and Professional Practice Group and was the National Partner-in-Charge for Quality Measurement.

26. As a result of, among other things, aspects of the conduct described herein, Britt, Holder, Marcello, Middendorf, Sweet and Whittle were each separated from KPMG sometime after approximately February 2017.

KPMG's Attempts to Remedy Its Poor Performance in Inspections

27. In or about 2015, KPMG was in the process of addressing concerns raised by the PCAOB concerning the firm's timeliness in responding to written comments relating to PCAOB engagement inspections, as well as the sufficiency of resulting audit documentation remediation. In particular, KPMG was focused on improving its performance with respect to the large number of banking engagements which had received written comments related to the auditing of loan and lease losses ("ALLL"), among other matters.

28. Beginning in approximately 2015, KPMG took various steps in an effort to improve its inspection performance. Such steps included, but were not limited to:

- a. Recruiting PCAOB employees, including Sweet and Holder.
- b. Retaining Palantir, a data analytics firm, to assist in predicting which engagements would be inspected.
- c. Implementing a financial bonus incentive system for members of audit teams which received no comments.
- d. Implementing an ALLL Monitoring program to add an additional level of review to KPMG's auditing of the accounting of "loan and lease losses."

Dissemination of Inspection Lists

2015

29. According to information provided by counsel to KPMG concerning their interviews of Brian Sweet,² I know the following:

a. Prior to leaving the PCAOB, Brian Sweet made a copy of his computer hard drive, which contained thousands of PCAOB documents, including, for example, internal planning documents and non-public comment forms. After beginning employment at KPMG, Sweet transferred these PCAOB documents to his KPMG laptop computer. Sweet also took hard copies of certain PCAOB documents, including a non-public list of engagements that had been selected for inspection in 2015 (the “2015 List”) from the PCAOB.

b. In approximately May 2015, during his first week of employment at KPMG, Sweet had lunch with Middendorf and others. During lunch, Middendorf asked Sweet to disclose information about which KPMG engagements would be inspected by the PCAOB. Middendorf also told Sweet to remember where Sweet’s paycheck came from.

c. Also during his first week of employment at KPMG, Brian Sweet had lunch with Whittle and Hermann. During lunch, Whittle asked Sweet which KPMG engagements would be inspected that year. During the same conversation, Whittle told Sweet that Sweet was most valuable to the firm at the present moment and that soon Sweet would be less valuable. Sweet

² With regard to the contents of interviews conducted by KPMG Counsel of current or former KPMG employees, KPMG has made clear that it has not intended or elected to waive the attorney-client privilege to the extent the privilege applies to such interviews. Instead, KPMG Counsel has relayed the information or answers that they “hypothetically” believe a particular witness would provide. Additionally, in certain cases, the description of events attributed to a particular witness varies from, or is contradicted by, the account attributed to another witness. Where facts are attributed to one witness, the different or contradictory account of another witness is not included herein.

understood this to mean that his knowledge of present PCAOB inspection activity was one of the primary “values” he brought to KPMG.

d. On or about Friday, May 8, 2015, at the end of Sweet’s first week of employment at KPMG, Sweet provided a copy of the 2015 List to Whittle. Whittle shared the list with other KPMG personnel, including Middendorf.

2016

30. Based on information provided by counsel for the PCAOB and KPMG Counsel concerning their interviews of Holder, I know the following:

a. Holder was close friends with Wada while at the PCAOB and remained so following her departure from the PCAOB.

b. In March 2016, Holder received a telephone call from Wada in which he told her to “write this down” and proceeded to provide her with a list of stock ticker symbols. The list of ticker symbols was the list of KPMG issuers to be inspected in 2016 (the “2016 List”).

c. Holder subsequently called Sweet and told him about her call with Wada. Sweet told Holder that Sweet would tell Whittle about the call from Wada.

d. Sweet called Holder back that same day and told her that he had discussed the list with at least Whittle, Britt and Middendorf. Sweet told Holder that Sweet had been told that the information was “too good to pass up” and Sweet directed Holder not to share the information with anyone else.

31. Based on information provided by KPMG Counsel concerning their interviews of Sweet, I know that on or about March 28, 2016, Sweet spoke to Whittle, Middendorf and Britt by phone. During that conversation, Sweet told Whittle, Middendorf and Britt that he had obtained a list of banks to be inspected from a colleague at the PCAOB. During the conversation they agreed

to use an existing monitoring system for ALLL-related issues to re-review work papers for the bank audits subject to inspection. In order to avoid alerting anyone to their possession of the inspection list, they agreed to notify all of the engagements teams with issuers included in the ALLL monitoring system, rather than only those on the list of issuers selected for inspection. Following that conversation, Britt arranged for Sweet, Holder, and several others to be given access to the audit files in the ALLL system in order to conduct “on top monitoring” of the relevant audits.

32. Based on information provided by KPMG Counsel concerning their interview(s) of Middendorf, on or about March 28, 2016, following the conversation described above, Middendorf notified Marcello that Sweet had acquired information concerning PCAOB inspections from an anonymous PCAOB source.

33. Based on information provided by KPMG Counsel, I know that, in connection with the “on top monitoring” done in connection with the receipt of the 2016 List, KPMG discovered an error in an aspect of KPMG’s audit of company called Ambac. At the time the error was discovered, an Ambac opinion had already been issued. As a result of discovering the error, KPMG withdrew its opinion with respect to internal controls.

2017

34. Based on my review of emails and text messages and information provided by KPMG Counsel concerning their interviews of Sweet, among others, I know the following:

35. On or about January 9, 2017, Wada and Holder spoke by cellphone. Shortly after the call, Holder called Sweet and told Sweet that Wada had provided her with the names of certain banks that were at high risk to be selected for inspection as well as certain audits of other issuers that were raising red flags (the “2017 Preliminary List”). Sweet then relayed the information to

both Whittle and Britt. Sweet understood that Whittle would share the information with Middendorf.

36. On January 10, 2017, one day after providing Holder with confidential PCAOB information, Wada emailed his resume to Cindy Holder.

37. On or about January 10 and January 11, 2017, Sweet reached out to a number of KPMG engagement partners to set up a time to speak. During those communications – and based on the information provided by Wada – Sweet told the engagement partners that he believed their respective engagements would be inspected.

38. On or about February 3, 2017, Holder and Wada again spoke via cellphone.

39. Shortly after the end of that call, Holder spoke to Sweet by phone. During the call, Holder provided Sweet with a list of 47 stock ticker symbols corresponding to 47 engagements which would be inspected in 2017 (the “2017 List”). Sweet wrote down the list. Sweet then spoke separately to both Britt and Whittle and provided each of them with the 2017 List.

40. On or about February 6, 2017, Sweet, Whittle and Middendorf spoke by phone and discussed the 2017 List. Middendorf copied down the list and said he would speak to Marcello about it.

Sweet Maintains Relationships at the PCAOB

41. Based on my review of email communications and information provided by KPMG Counsel concerning its interviews of Sweet, I know that after leaving the PCAOB, Sweet remained in contact with many then-current PCAOB employees, including but not limited to, Grady Peeler, Matt Sickmiller, Robert “Bob” Ross, Steven Schindler, David Knibbs, Karen Tyler, Jeffrey Watkin, Duane Abel, and August Bellome. Among other activities, Sweet stayed in email communication with PCAOB employees, participated in a “fantasy football” league with PCAOB

employees, and met PCAOB employees for meals and drinks. During some of these interactions, Sweet attempted to learn confidential PCAOB information from then-current employees. On at least one occasion, following a meal with a PCAOB employee, Sweet made notes of the conversation to remind himself of the information he had learned.

Recruitment Efforts

42. Between at least 2014³ and 2017, with the involvement of Britt, Marcello, Middendorf, Whittle, and others, KPMG recruited, and in some cases, hired PCAOB employees. After Sweet and Holder were hired by KPMG, they each participated in communications with other then-current PCAOB employees about the possibility of employment at KPMG.

43. Between at least 2014 and 2017, then-current PCAOB employees, including but not limited to Sweet, Holder, Hector Santana, Jeffrey Wada, Jung Lee, David Knibbs, Jeffrey Peeler, and James Teter (i) engaged in discussions with KPMG personnel about possible employment; (ii) provide their respective resumes to KPMG personnel; and/or (iii) were in fact hired by KPMG.

44. In several instances, PCAOB employees provided draft resumes to Sweet or Holder for review and/or provided resumes to Sweet for the purpose of having the resumes passed to KPMG.

Other Improper Uses of Confidential PCAOB Information

45. Based on my review of email communications and information provided by KPMG Counsel concerning its interviews of Sweet and Holder, among others, I know that in addition to disclosing and passing on lists of engagements to be inspected in 2015, 2016, and 2017, Brian

³ Efforts to recruit Sweet began in at least September 2014.

Sweet also disclosed confidential PCAOB information to his colleagues at KPMG for use in other ways. For example:

a. In or about May 2015, at Sweet's request, and while still employed at the PCAOB, Holder sent Sweet an internal PCAOB document summarizing various deficiencies at KPMG, for the purpose of assisting Sweet in preparing for a meeting at KPMG concerning firm deficiencies.

b. In or about 2015, KPMG contracted with Palantir, a data analytics service, to assist in efforts to predict which KPMG engagements would be the subject of PCAOB inspections. Sweet provided KPMG personnel responsible for the Palantir project with a list of confidential PCAOB "risk factors," which would make an engagement more likely to be inspected.

c. In or about 2016, Dabie Tsai, a KPMG partner, was engaged in efforts to secure as a KPMG client a Spanish bank, BBVA. Sweet provided Tsai with confidential PCAOB comments concerning another GNF auditing firm's audit of a different Spanish bank in order to assist her in landing BBVA as a KPMG client. Tsai was ultimately successful and BBVA became a KPMG client.

Efforts to Conceal the Illicit Receipt of PCAOB Information

46. Based on information provided by KPMG Counsel concerning their interviews of Sweet, I know that on or about February 14, 2017, Sweet called Holder. During the conversation, Sweet and Holder discussed the fact that KPMG's Office of the General Counsel was investigating the improper receipt of confidential PCAOB information by KPMG employees. Sweet and Holder discussed covering up the receipt of information from Wada by falsely telling the Office of the General Counsel that Holder had received the confidential PCAOB information from an anonymous letter.

47. Based on information provided by KPMG counsel concerning their interviews of Holder, emails between Holder and Whittle, and my review of text messages obtained by KPMG counsel from a cellphone affiliated with Holder, I know the following:

a. In or about February 2017, Holder deleted text messages between herself and Wada concerning Wada's having provided her confidential PCAOB information. Notwithstanding this attempted deletion, KPMG counsel was able to recover text messages between Holder and Wada concerning Wada's having provided Holder confidential PCAOB information.

b. On or about February 16, 2017, Whittle emailed Holder asking her to call him. During a subsequent conversation, Whittle told Holder that "we never talked about the list" and she responded, "right."

B. Probable Cause Regarding the Subject Accounts

48. Based on my review of emails produced by Sweet, Holder and/or Wada from the Sweet, Holder and Wada Accounts in connection with the internal investigations conducted by KPMG and/or PCAOB counsel, I know the following:

The Sweet Account

49. On or about April 24, 2015, his last day at the PCAOB, Sweet sent an email from his PCAOB account to a long list of PCAOB employees to say farewell and to provide his contact information. In the email he provided the Sweet Account as his email address.

50. On or about May 5, 2015, Sweet used the Sweet Account to email Holder at the Holder Account saying, "I've got a meeting set up with the head of the group tomorrow and pulled together a list of potential hires (along with Joe Lynch) and put you as the #1 target!!!![] I really think we can make this work, and am very optimistic. I'll fill you in after the convo tomorrow."

51. That same day, Sweet used the Sweet Account to separately email both David Knibbs and Grady Peeler, who were then both current PCAOB employees. Sweet said that Sweet was

meeting with KPMG personnel the following day to discuss individuals KPMG should hire, including Knibbs/Peeler. Sweet asked for a resume and said to call him on his cellphone with any questions.

52. On or about May 12, 2015, David Knibbs emailed the Sweet Account attaching Knibb's resume. Sweet then forwarded the email to Sweet's own KPMG email address. The following day Sweet used the Sweet Account to email Knibbs providing comments on Knibb's resume and telling Knibbs that Sweet could get "get it [the resume] in front of the group lead partner today."

53. On or about May 12, 2015, Holder used the Holder Account to email the Sweet Account with the subject line, "Anonymous email." Attached to the email was an internal PCAOB Part II deficiencies comment form for KPMG, which contained "comment bubbles" reflecting the thoughts of certain PCAOB personnel. As referenced above, based on information provided to KPMG counsel by Holder, I know that at the time Holder sent this email, Sweet was preparing for a meeting with other KPMG personnel to discuss the firm's deficiencies.

54. On or about May 28, 2015, James Teter – a PCAOB employee – emailed the Sweet Account to ask if Sweet had had a chance to check in about Teter's efforts to obtain employment at KPMG.

55. On or about May 30, 2015, Grady Peeler – a PCAOB employee – emailed the Sweet Account attaching a copy of Peeler's resume.

56. On or about June 22, 2015, Hector Santana – a PCAOB employee – emailed the Sweet Account to tell Sweet that Santana would be interviewing at KPMG and to ask if Sweet had time to give him any advice. Sweet responded directing Santana to call Sweet on Sweet's cellphone. Santana was subsequently hired by KPMG.

57. On or about April 8, 2016, Jung Lee – a PCAOB employee – emailed both the Sweet Account and Sweet’s KPMG email account and attached a copy of Lee’s resume.

58. On or about April 15, 2016, Sweet used the Sweet Account to email Jung Lee providing proposed edits to Lee’s resume. In the email, Sweet said that Lee should send the resume back when it is done and Sweet would “start spreading it around.” Sweet noted that “I’ve had a few conversations with folks already and its [sic] gone really well so I think there will be a lot of interest.”

59. On or about April 6, 2016, Dabie Tsai used her KPMG email account to email Sweet on his KPMG email account to thank him in advance for his help and to say she would send a meeting invite for them to discuss the “two Spanish banks we discussed just now.” Tsai also provided Sweet with her personal email account and fax number “in case you want to use either.”

60. On or about April 8, 2016, Sweet used his KPMG email account to email Tsai at her KPMG email account and provided a publicly available PCAOB report.

61. Shortly thereafter, Sweet used the Sweet Account to email Tsai’s personal account (the “Tsai Account”) and said, “Dabie, it was great chatting with you today! Attached are some examples of the types of issues that have been raised in the past.” Attached to the email was an internal PCAOB comment form for Banco Santander, a Spanish bank.

62. That same day, Tsai used the Tsai Account to respond to the Sweet Account saying “Thank YOU so much!!!! I have printed each out so it will only be on the hard copy that I read . . . I promise to take appropriate care of this. Appreciate all of your help - and I am sure you’ve heard it many times, but I am going to add it to all the other accolades - I am so glad you came to KPMG – you’ve been a huge help to the firm . . . since you joined!. . . I’ll be in touch re: our current proposal effort.”

The Holder and Wada Accounts

63. In addition to the emails to and from the Holder and Wada Accounts set forth above, the following emails were also sent or received from the Holder and Wada Accounts:

64. On or about March 1, 2016, Wada received an email on his PCAOB email account announcing the promotions of various PCAOB employees. Wada was not among the employees who had received a promotion. Later that day, Wada forwarded the email to the Wada Account. Wada also forwarded the email to the Holder Account. Holder then forwarded the email to the Sweet Account.

65. On or about January 10, 2017, one day after providing the 2016 Preliminary List to Holder, Wada emailed Holder on the Holder Account saying “It’s funny how I was on the fast track to partner and clearly recognized for my talents at Deloitte and then I end up in this [expletive] place with all the [expletive] politicking that I loathe and now I can’t get a goddamn promotion to save my life just because I refuse to kiss people’s [expletive] and spread the political rhetoric. God this place sucks. Please let me know what else you need from me.” Wada attached his resume to the email.

Preservation of the Subject Accounts

66. On or about April 21, 2017, a preservation request pursuant to 18 U.S.C. §2703(f) was sent to Yahoo!, Inc. directing the preservation of the Sweet Account.

67. On or about April 26, 2017, a preservation request pursuant to 18 U.S.C. §2703(f) was sent to AOL and Google, Inc. directing the preservation of, respectively, the Holder and Wada Accounts.

C. Evidence, Fruits and Instrumentalities

68. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers’ servers associated with the Subject Accounts for the time

period January 1, 2014 up to and including the date of this Affidavit will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrants.

69. In particular, I believe the Subject Accounts are likely to contain the following information:

- evidence of any efforts to obtain, embezzle, misappropriate, transfer, share or exploit confidential information obtained by virtue of employment at PCAOB (“confidential PCAOB information”), and evidence of any agreement to do the same;
- evidence of communications concerning efforts by PCAOB employees to obtain employment outside of PCAOB, including, but not limited to employment at KPMG;
- evidence of any motive to obtain or share confidential PCAOB information, including, but not limited to, financial motives, personal relationships, or job dissatisfaction;
- evidence of the nature of the relationships between the users of the Subject Accounts and their relationships with current and former-PCAOB employees;
- evidence of efforts to destroy evidence, delete emails or text messages, make misleading statements or craft false explanations concerning the obtaining, possession, transfer, sharing or utilization of confidential PCAOB information;
- email header information (which can place the users of the Subject Accounts or their confederates at a certain time and place);
- geographic location of user, computer, or device (the content and header information can both indicate that the email was communicated through a particular physical location; metadata from photo attachments can reflect geographic location)

- locations of the users of the Subject Accounts and the identities and locations of their confederates, as well as anyone knowingly or unknowingly used as an intermediary in the obtaining or sharing of confidential PCAOB information (including email communications, photos or other attachments, and address book information)
- location of other evidence (*e.g.*, emails reflecting registration of other online accounts potentially containing relevant evidence); and
- passwords or other information needed to access the account users' computer or other online accounts.

III. Review of the Information Obtained Pursuant to the Warrants

70. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrants.

71. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails and evidence within the Subject Accounts. This

method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

72. The scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrants could alert potential criminal subjects or targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that subjects and targets of the investigation are known to use computers and electronic communications in furtherance of their activity, such subjects and targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.


73. Accordingly, there is reason to believe that, were the Providers to notify the subscribers or others of the existence of the warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Providers

not to notify any person of the existence of the warrants for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

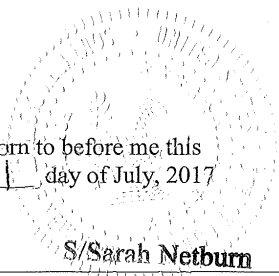
74. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrants and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

75. Based on the foregoing, I respectfully request that the Court issue the warrants sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.


LYESON DANIEL
Postal Inspector
United States Postal Inspection Service

Sworn to before me this
21 day of July, 2017


S/Sarah Netburn
HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York